



KCJIS NEWS

NOVEMBER 2014

NEWS FROM BIOLOGY CASEWORK

JOHN GAUNTT, KBI, BIOLOGY SECTION

As of November 1st, when your agency submits evidence for biology testing to any of the KBI laboratories, a DNA submission form must accompany the evidence submission process. The submission form and the biology case submission guidelines were made available to agencies August 1st. The Evidence Control Centers gave agencies until November 1st to acclimate to the new process.

The Evidence Control Centers have forms available in case an officer forgets to bring this form with the evidence items. Cases will not be accepted by the Evidence Control Centers unless the form with case synopsis is completed.

The DNA submission form and biology submission guidelines are available on the KBI website http://www.kansas.gov/kbi/info/info_forms.shtml and on the Kansas Criminal Justice Information System (KCJIS) site at <https://www.kcjis.state.ks.us/SitePages/Forms.aspx>

If you have any questions, please contact any of the KBI Evidence Control Centers for assistance.

INSIDE THIS ISSUE:

NEWS FROM BIOLOGY	2
EXPUNGEMENT PROCESS	2
REMEMBER TO BE VIGILANT	2
KCJIS PATCHING	2-3
OFFSITE SHREDDING	3-4
FROM 911 TO COURTROOM	4-5
ADVANCED AUTHENTICATION	5-6
HELPDESK NEWS	6-9
R.A.P.I.D	9-11
CIVIL FAILURE TO APPEAR	11
NEWSLETTER CONTACT	11



DNA Submission Form

Kansas Bureau of Investigation

1420 SW Tyler
Topeka, KS 66612
(785) 236-4000

7250 State Ave.
Kansas City, KS 66112
(913) 286-4540

625 Washington
Great Bend, KS 67530
(620) 782-4104

When evidence is submitted with a Biology/DNA exam request, this form must be fully completed in addition to the Evidence Custody Receipt. Otherwise, evidence testing may be delayed until the completed form has been received by the laboratory.

Case Information

Contributing Agency	Agency Case #	KBI Case # (if known)
Investigating Officer	Phone	E-Mail
Has any evidence been previously submitted on this case by any agency? <input type="checkbox"/> Yes <input type="checkbox"/> No		
Is a synopsis included (page 2) or investigative report attached? <input type="checkbox"/> Yes <input type="checkbox"/> No		

References

If known reference standards are not received with the original submission of evidence it may delay analysis or evidence may be returned until the known reference standards are obtained.

	Name (Last, First)	Sample Type	Known collected?	Reason Not Collected
1		Victim <input type="checkbox"/> Suspect <input type="checkbox"/> Other <input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2		Victim <input type="checkbox"/> Suspect <input type="checkbox"/> Other <input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3		Victim <input type="checkbox"/> Suspect <input type="checkbox"/> Other <input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4		Victim <input type="checkbox"/> Suspect <input type="checkbox"/> Other <input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5		Victim <input type="checkbox"/> Suspect <input type="checkbox"/> Other <input type="checkbox"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Evidence

Evidence will be analyzed using a priority based system. List the priority of your evidence for analysis (1 = highest, 10 = lowest)

Item #	Evidence Description	Source/Specific Location of Evidence (Ex - Suspect's House, Victim's Car, Crime Scene)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Synopsis

The KBI must evaluate and document all evidence for potential upload to CODIS. A synopsis is required to aid in this process.

NEWS FROM BIOLOGY CASEWORK—CONTINUED

JOHN GAUNTT, KBI, BIOLOGY SECTION

News from the DNA Databank:

Short and sweet: the Databank receives approximately 220 samples each week to process and upload into CODIS (Combined DNA Index System) for comparison to unsolved crimes across the country. If there is a match, we call it a CODIS hit.

A CODIS hit tells the investigating agency that a crime scene item of evidence has the same DNA profile as an offender. This information can be used as probable cause to locate the offender and collect a DNA swab. Since the Databank sample used in the CODIS search was not collected as evidence and has no chain of custody, the laboratory requires an evidence DNA sample (blood tube or oral swab) for comparison to the crime scene evidence.

Booking centers should understand that any DNA Databank sample could solve a homicide, a sexual assault, or a property crime that would remain unsolved if that DNA sample would not have been collected. This is an awesome opportunity to solve a crime.

We thank all of the booking centers across Kansas for doing a great job.

EXPUNGEMENT PROCESSING

VANESSA RINE, KBI, CRIMINAL HISTORY RECORDS UNIT

In recent days, the Kansas Bureau of Investigation (KBI) has received a larger than normal quantity of rejected expungements from the Federal Bureau of Investigation (FBI). The expungements were rejected because they were mailed directly from the court to the FBI and did not come from the KBI Central Repository. The FBI requires expungements to be processed by the KBI Central Repository then sent to the FBI electronically.

To ensure the expungements are processed in a timely manner, please send them to the KBI Central Repository for processing. The KBI is then required by statute to forward a copy of the expungement to the FBI, proper arresting agencies, and the Kansas Department of Corrections (KDOC) for those agencies to expunge their records. If you have any questions you can contact Vanessa Rine at 785-296-0816.

REMEMBER—ALWAYS BE VIGILANT

DON CATHEY, KHP, KCJIS INFORMATION SECURITY OFFICER

How much do you use email and the internet to conduct your work and personal business?

What current events do you use the internet to follow?

In a recent alert, the United States Computer Emergency Readiness Team (US-CERT)* reminds us to protect against email scams and cyber campaigns. This link offers some preventative measures to protect ourselves. How many are YOU already following?

<https://www.us-cert.gov/ncas/current-activity/2014/10/16/Ebola-Phishing-Scams-and-Malware-Campaigns>

* The US-CERT website <https://www.us-cert.gov/> contains links to other publications and security resources. The **ALERTS and TIPS** page offers subscription services that can help you meet the FBI CJIS policy requirement that agencies **receive information system security alerts/advisories on a regular basis** (5.10.4.4 Security Alerts and Advisories).

KCJIS PATCHING POLICY & PRACTICE

KIP BALLINGER, KHP, KCJIS TECHNICAL SECURITY AUDITOR

KCJIS security policy requires that agencies develop and implement a local policy regarding the timely patching of the various components on agency networks where Criminal Justice Information is processed or stored. Beyond simply having a policy in the Standard Operation Procedures (SOP), the agency must actively ensure it is being done.

Continued on page 3

KCJIS PATCHING POLICY & PRACTICE—CONTINUED

KIP BALLINGER, KHP, KCJIS TECHNICAL SECURITY AUDITOR

When you hear the word 'patch', what comes to mind... something you iron on the knee of your old jeans?; something you wear after an eye injury? The word 'patch' as it is used in KCJIS policy, can be misleading as it tends to be industry jargon. For the purposes of policy, it is to be understood synonymously as 'updating' or applying updates / fixes / patches etc. to both software programs and hardware (firmware / operating system). There are different types of patches, such as: point patches / hotfixes, bundled patches, and version releases.

The current patch management language came into version 5.0, starting in Feb. 2011. Current KCJIS Policy area 5.10.4.1 states in part that:

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes.

Local policies should include such items as:

- Testing of appropriate patches before installation.
- Rollback capabilities when installing patches, updates, etc.
- Automatic updates without individual user intervention.
- Centralized patch management.

The patching requirements first appeared in FBI CJIS Security policy Version 4.0 in September of 2004 and was specific to the firewall (network border device). At that time, policy section 7.10 - Firewalls stated that, "Any appropriate operating system patches shall be applied before any installation of firewall components, and procedures shall be developed to ensure that the firewall patches remain current while the firewall retains its statefulness."

Policy now applies to everything used to access or process Criminal Justice Information (CJI).

While earlier this year we saw an emphasis regarding the 'End of Life' for the Windows XP operating system, we need to remember that the patch policy also applies to software applications and your network appliances, too.



OFF SITE SHREDDING—A KCJIS CASE STUDY

TAMMIE HENDRIX, KHP, KCJIS TECHNICAL SECURITY AUDITOR

An agency has a company that shreds their paper Criminal Justice Information (CJI). They do NOT destroy it on site, but send a certificate each time they shred as proof of destruction. What needs to happen for policy compliance?

This scenario demonstrates one form of indirect access by a private contractor.

Here are the policy areas to review for this scenario:

- 3.2.7 Agency Coordinator (AC)
- 5.1.1.5 Private Contractor User Agreements & CJIS Security Addendum
- 5.2 Security Awareness
- 5.8.2 Media Transport
- 5.8.4 Disposal of Physical Media
- 5.9.1.3 Physical Access Control
- 5.9.1.8 Delivery & Removal
- 5.12.1 Personnel Security

Continued on page 4

OFF SITE SHREDDING—A KCJIS CASE STUDY—CONTINUED

TAMMIE HENDRIX, KHP, KCJIS TECHNICAL SECURITY AUDITOR

1. The agency will need to execute a contract that includes by reference the FBI CJIS Security Addendum. (See Appendix H of the Policy).
 - a. Each person at the shredding company authorized to handle the hard copy CJI will need to sign the FBI CJIS Security Addendum Certification page.
2. Someone at the agency will need to act as the Agency Coordinator.
3. The shredding company will need to provide a list of who will be responsible for access to the hardcopy in their bins and coordinate with the agency to get them “authorized.”

Policy area 5.8.4 says; “... Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.”

The FBI CJIS Security Policy includes this definition:

“Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to Criminal Justice Information (CJI).

From policy area 5.12.1.2:

“Prior to granting access to CJI, the Contracting Government Agency (CGA) on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.”

The agency will also need to do annual name based rechecks per KCJIS policy.

4. The agency will need ensure that those contracted employees also complete basic security awareness training as listed in policy area 5.2.1.1 for All Personnel.

A review of agency systems, processes and retention policies may reveal ways to reduce the need for bulk hardcopy destruction. You may also want to consider the annual costs and benefits of buying a shredder for CJI shredding.

FROM 9-1-1 TO THE COURTROOM

JESSICA DOMME, ATTORNEY GENERAL’S OFFICE

Each year, the Criminal Division of Kansas Attorney General Derek Schmidt’s Office provides statewide training on domestic violence at four regional locations for prosecutors, law enforcement and allied professionals. The Kansas Attorney General’s Office offers the training through funding provided from federal S.T.O.P. (Services, Training, Officers, Prosecutors) grant funds awarded by the Kansas Governor’s Grants Program, through the Office of Violence Against Women, U.S. Department of Justice. This year, the Kansas Attorney General’s Office coordinated with the Governor’s Advisory Council on Domestic Violence Training to present “From 9-1-1 to the Courtroom: A Coordinated Response to Domestic Violence.” The purpose of the multi-disciplinary training is to create a consistent, coordinated response to domestic and sexual violence from the time of a 911 call reporting an incident, through the investigation, arrest, prosecution, probation or parole and release of offenders.

The Governor’s Advisory Council on Domestic Violence Training is a partnership between the Kansas Governor’s Office and the Kansas Coalition Against Sexual and Domestic Violence (KCSDV), the Kansas Law Enforcement Training Center (KLETC), the Kansas Attorney General’s Office, the Kansas Office of Judicial Administration, the Kansas Department of Corrections, and many local agencies to create comprehensive training curricula for professionals in the criminal justice system who respond to domestic violence and sexual assault.

Continued on page 5

FROM 9-1-1 TO THE COURTROOM—CONTINUED

JESSICA DOMME, ATTORNEY GENERAL'S OFFICE

This training effort is funded through a Federal Grant to Encourage Arrest Policies and Enforcement of Protection Orders Program (GTEAP) by the Office on Violence Against Women, U.S. Department of Justice. The curricula developed through the grant provides comprehensive, up-to-date information to address basic, as well as new and emerging issues, and moves beyond information-based training towards building skills.

"From 9-1-1 to the Courtroom" is developed specifically for prosecutors, law enforcement officers, system and community based advocates, batterers intervention program staff, communications specialists, probation and corrections officers, and all allied professionals working within the criminal justice system. The training is provided at no cost to attendees. Training topics include batterer motive, victim dynamics, law enforcement arrest considerations, victim safety and data collection, and legal ethics for attorneys prosecuting domestic violence cases. The training has been held in Leavenworth, Hays, and Garden City. On December 10, 2014, the training will be held at Memorial Hall in Independence, Kansas. Those interested in attending the training can apply for registration online at www.ag.ks.gov/dv-seminar. For further information contact Jessica G. Domme, Assistant Attorney General, 785-296-2215.

ADVANCED AUTHENTICATION UPDATE

DON CATHEY, KHP, KCJIS INFORMATION SECURITY OFFICER

Are you familiar with the saying "the more things change, the more they stay the same?"

Well, when it comes to the CJIS security policy regarding Advanced Authentication, this phrase seems to apply in Kansas.

As recently as August of this year, the FBI CJIS security policy required Advanced Authentication (AA) - that is using two of the three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric) - when accessing Criminal Justice Information from outside a physically secure location.

FBI had allowed interim compliance with some stipulations *"for users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2014...."*

Furthermore, KCJIS policy Part II states *"...a RSA SecureID token (ordered from Fishnet Security under state contract) must be used for Advanced Authentication to KCJIS resources"*.

The "more they change" part:

The FBI CJIS Security Policy version 5.3 was released August 4, 2014. It is available for all to read at <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>. There are notable changes in this policy that affect the AA discussion.

1. Policy area 5.9.1 changed the definition of a physically secure location to include a police vehicle where access can be controlled.

*"A physically secure location is a facility, **a police vehicle**, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems"*

A police vehicle is any conveyance that can be locked and otherwise control who gets in them when a device may be processing CJI. A horse, bicycle, motorcycle, Segway, etc. still are NOT physically secure.

2. The FBI defined a new term "Indirect Access" to be *"Having the authority to access systems containing CJI **without providing the user the ability to conduct transactional activities** (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories)."*
3. They also changed the language within policy area 5.6.2.2.1 Advanced Authentication Policy and Rationale to read:

*AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), **or when the user has no ability to conduct transactional activities on state and national repositories**, applications, or services (i.e. indirect access).*

ADVANCED AUTHENTICATION UPDATE—CONTINUED

DON CATHEY, KHP, KCJIS INFORMATION SECURITY OFFICER

4. Policy Area 5.6.2.1.2 Personal Identification Number (PIN) was expanded to make what was the Appendix G-5 recommendations actual policy for PINs. Most notable on the list – a minimum length of 6 digits. (KCJIS will develop a plan to gradually transition existing users to these new minimum requirements).

The “stay the same” part:

Meanwhile, an RSA SecureID token must still be used for accessing KCJIS resources such as the central message switch for NCIC, III queries and entry or to access the KCJIS portal. This requirement is built into our current KCJIS system and cannot be changed for now.

What does this all mean?

It means the Advanced Authentication requirements are being met in Kansas. (NO DIRECT access to CJ is possible without the two factors of PIN + TOKEN). Therefore, you can disregard any sales pitches in regards to the September 30th deadline to be compliant with AA policies.

Agencies may develop authentication policies for access to their local systems if they desire. However, keep in mind that KCJIS currently requires the RSA token but that the KBI has initiated a Security Architecture Modernization project which will provide, among other things, a federated solution¹. When asked for comment, Joe Mandala, Chief Information Officer at the KBI, offered this:

“The KBI project may very well include options to the RSA token, based on agency feedback. KCJIS welcomes local input for this and any other ideas you may have for improvement.

While KCJIS and the KBI will continue doing everything that we can to provide as flexible of architecture as possible as an outcome of this project, there are two things that are critical to its success. One is, as stated above, input from participants in the system – you and other partner agencies. We need to know what you need. The other is funding; what you need from us dictates the cost to provide it. While the KBI has in the past provided the funding for the security architecture for KCJIS, and partner agencies have provided the funding for their own tokens, that cost model will likely change if a newer and more flexible architecture is adopted. Minimizing cost and maximizing usability is our goal; we need your help to achieve both”

Meanwhile, when it comes to Advance Authentication and KCJIS, everyone just needs to “keep on, keepin’ on.”

¹ In 2005, the US Departments of Justice and Homeland Security began sponsorship of a concept called Global Federated Identity and Privilege Management (GFIPM) which seeks to develop secure, scalable, and cost-effective technologies for information sharing within the law enforcement and criminal justice communities.

NEWS FROM THE KBI HELP DESK

JAVIER BARAJAS, KBI, HELPDESK

Delivery of Multiple CCH Responses

In May of 2014 the KBI Help Desk received a call reporting when a Kansas Car Stop (KCS) is submitted with the License Plate (LIC) information for a Colorado tag the KCS response from Colorado via NLETS that says “not on file.” However, when an Vehicle Query through NLETS (RQ) is ran they get a response back that has the registration information for the Colorado tag. After the KBI Help Desk performed troubleshooting steps, the issue was narrowed down to a switch function called aggregator. The purpose of aggregator is to return traffic from several data sources to the same requestor. This example is unique because two responses were sent to the KCJIS switch from NLETS instead of the typical single response. For a KCS request, before May of 2014 the behavior of aggregator expected only one response from each data source.

As of May 2014, Computer Projects of Illinois (CPI) adjusted the behavior of aggregator and now the requestor will receive all responses from each data source.

In summary, when the message switch receives multiple responses from a single data source (for example, NLETS) the requesting user will receive all responses from the same data source rather than a single response from each data source. In the Colorado tag example given above, the KCS was ran and because Colorado has two separate data sources they sent two separate responses to our Kansas switch via NLETS. Before CPI's adjustment the requestor will only receive the first response from NLETS and all other responses from NLETS will be ignored. Now that CPI's adjustment is in place, the requestor will receive all information from the Colorado data sources via NLETS.

Continued on page 7

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI, HELPDESK

Medical Certification Information

On May 20, 2014, Kansas Department of Revenue (KDOR) started returning Medical Certification Information on Kansas Driver's License Records for people who have a Commercial Drivers License (CDL). People with a CDL must self-certify to a single type of commercial operation. Based upon the commercial operation type they certify to, a current medical examiner's certificate may be required.

In the example below the Category (CAT:), Certification Code (CODE:), STATUS:, Examiner Specialty Code (SPC:), Restrictions (REST:), fields are highlighted as well as the name of the doctor who performed the examination. The subjects name is John Doe Brown and the doctor who performed the examination for John's certification is Dr. Jack Joe Smith.

ZQ90

BROWN JOHN DOE DOB/01011979 ROR IND/
SEX/M EYE/BLK HGT/500 WGT/200 IMG/P CCL STTS/ CCL EXP/00000000
STATUS: REG:VALID KANSAS CDL:VALID KANSAS SOC/123456789
OLN/KO1234567 TYPE/COMMERCIAL CLASS/ CDLCLASS/B PREV OLN/
ENDOR/N ISS/01012013 EXP/01012017 RENEWAL/06012013
123 W MAIN ST
BIG CITY KS 66000
RSTR:B :CORRECTIVE LENSES :
CAT:1 CODE:NI STATUS:C EXAM:01012013 ISSUE:01012013 EXPIRE:01012015
SPE EFF:00000000 SPE EXP:00000000 WVR EFF:00000000 WVR EXP:00000000 JRS:KS
SPC:AN EX NMB:74166 TEL:7852968245 REG:
REST:CORR LENSES/
LAST NAME:Smith SFX: Dr.
FIRST:Jack MID: Joe
NO HISTORY FOR THIS OPERATOR
NO ALIAS FOR THIS OPERATOR
*** CRIMINAL JUSTICE USE ONLY - DO NOT DISSEMINATE ***

Below you will find the new fields and their applicable values that will be displayed for people with a CDL. (See example above)



Continued on page 8

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI, HELPDESK

Category (CAT:)

☐ Category 1 = NI

☐ Category 2 = EI

☐ Category 3 = NA

☐ Category 4 = EA

Certification Code (CODE:)

☐ NI = Non-Excepted Interstate

☐ EI = Excepted Interstate

☐ NA = Non-Excepted Intrastate

☐ EA = Excepted Intrastate

Status (STATUS:)

- C = Certified
- N = Not Certified

Examiner Specialty Code (SPC:)

☐ AN = Advanced Practice Nurse

☐ CH = Chiropractor

☐ DO = Osteopathic Doctor

☐ MD = Medical Doctor

☐ PA = Physician Assistant

Restrictions (REST:)

☐ CORR LENSES = Corrective Lenses in CMV

☐ HEARING AID = Hearing Aid in CMV

☐ WAIVER = Accompanied by waiver/exemption

☐ EXPT 391.62 = Driving exempt 49 CFR 391.62

☐ ACCPT SPE = Accompanied by SPE

☐ CFR 391.64 = Qualified under CFR 391.64

A complete list of values has been added to the KCJIS Web Portal. Click on the Information tab and click the link titled 'Kansas Driver's License Return Field Definitions 2014-03-26' under the KDOR section of the KS State Systems heading.

New KCJIS Web Portal

In July of 2014 on behalf of KCJIS, the KBI IT pushed out a new and updated version of the KCJIS Web Portal. The new Web Portal version comes with more functionality and ability to adjust to future KCJIS needs. KBI Help Desk staff held training sessions in Topeka Oct 14 – 16 and in Hays Sept. 16. The next opportunity for training will be at the KCJIS Conference in Topeka.

Continued on page 9

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI, HELPDESK

Gordon.lansford@ks.gov'." data-bbox="143 224 619 451"/>

The KCJIS Committee welcomes suggestions from the KCJIS User community regarding topics and presenters that you would like to see at this year's conference. Please submit your ideas to Gordon Lansford at Gordon.lansford@ks.gov

Annual KCJIS Conference:

*June 7 – 9, 2015
Ramada Inn Hotel,
Topeka, KS*

KCJIS Web Portal – DL Photos

As a reminder, the purpose of the Drivers License (DL) Photo function on the Web Portal is solely for getting the Name / DOB and Photo. Any other information needed on a subject should be obtained by running the appropriate message key through the Central Message Switch or using the Master Search via the subjects DL Number.

R.A.P.I.D—REPORT AND POLICE IMPAIRED DRIVERS

LAURA BOHNENKEMPER, KBI, HELPDESK

Status Report, 10 October 2014

The third quarter of 2014 saw an exciting event; the unveiling of the new KCJIS Portal and bringing the electronic disposition interface live. The new portal is stable and functioning well. The “shakedown” was minimal and the feedback from the KCJIS community was helpful. Certification of prosecutor and court disposition interfaces is in full swing and will be an ongoing process as entities create their interfaces. Work continues on the remaining data sources to be added to the Master Search and the Alerts.

Project Activity – through 2014 3rd Quarter

Work on the KCJIS Portal was completed and the new portal went live on August 5th.

Work continued with the first court to integrate with the Court Standard Interface for disposition reporting. Work continues to complete verification and testing on this initial court interface, and it is scheduled to go live in the 4th Quarter. While it has taken longer than initially estimated to complete this first court interface, resulting in a change order for schedule, the end result should be a solid operational interface.

Crash Master Enity Index (MEI) Integration, Detail Record Retrieval was completed. Test plans were completed and client testing of the Kansas Incident Based Reporting System (KIBRS) interface is in progress. Message Switch Notification Integration design documentation has been completed with development underway.

Project Change Order 10 was executed. This change order involved some modifications to the schedule to allow more time to work with courts in the certification process and to rearrange a few deliverables to mitigate encountered delays. Some enhancements were added to the change order to make the disposition process more efficient and to modify business rules requirements.

Continued on page 10

R.A.P.I.D—REPORT AND POLICE IMPAIRED DRIVERS—CONTINUED

LAURA BOHNENKEMPER, KBI, HELPDESK

Upcoming Project Activity

The coming quarter (2014 4th Quarter) will see Sub-Project 2.4: CRASH/KIBRS Integration very close to completion and Sub-Project 2.5: Message Switch Notification Integration ready for client testing.

Design work that will be completed in the next quarter includes:

- No Design Work scheduled in fourth quarter

Development work that will proceed during fourth quarter includes:

- Message Switch Notification Integration

Testing work for fourth quarter includes:

- Continuing certification of court and prosecutor interfaces (ongoing)
- KIBRS Integration Client Tests
- Message Switch Notification Integration - System Tests

The next quarter will be allocated to Court and Prosecutor interface certifications, adding message switch notifications for use with the Alerts and putting the final touches on the KIBRS data source.

Major Milestones

The following milestones were completed in the preceding reporting period:

- Crash and KIBRS Integration Test Plan was completed on July 9th
- CCH & Court Integration Client Test was completed on August 5th
- Crash MEI Integration, Detail Record Retrieval was completed on September 19th
- Message Switch Notification Integration - Design Documentation was completed on September 23rd
- Deliverables Completed

This is a list of deliverables completed and milestones reached in the reporting period. The "WBS Task #" column refers to a specific related task in the project plan. Note that some Task Numbers and Due Dates were modified by Change Request 10.

<i>Deliverable Name</i>	<i>WBS Task #</i>	<i>Due Date</i>	<i>Date Delivered</i>
KIBRS MEI Integration*	557	7/9/2014	4/23/2014
Crash/KIBRS Integration Test Plan	530	6/10/2014	7/9/2014
CCH & Courts Integration - Client Test	484	6/12/2014	8/5/2014
Crash MEI Integration, Detail Record Retrieval	546	8/26/2014	9/19/2014
Message Switch Notification Integration - Design Documentation	648	8/8/2014	9/23/2014
CCH/Court Integration Subproject Deployment	499	6/18/2014	10/7/2014

***Note:** this Deliverable was not due until 2014Q3 and was completed in 2014Q2

R.A.P.I.D—REPORT AND POLICE IMPAIRED DRIVERS—CONTINUED

LAURA BOHNENKEMPER, KBI, HELPDESK

Late Deliverables and Milestones

These deliverables were due in the reporting period, but have not been completed.

<i>Deliverable Name</i>	<i>WBS Task #</i>	<i>Due Date</i>

Upcoming Deliverables and Milestones

This is a list of deliverables to be completed and expected milestones to reach in the next reporting period.

<i>Deliverable Name</i>	<i>WBS Task #</i>	<i>Due Date</i>
KIBRS Integration - System Tests	611	10/3/2014
Message Switch Notification Integration - Test Plan	657	10/3/2014
Message Switch Notification Integration	662	11/18/2014
KIBRS Integrations - Client Tests	620	12/2/2014
Message Switch Notification Integration - System Tests	705	12/29/2014

CIVIL FAILURE TO APPEAR

LESLIE MOORE, KBI INFORMATION SERVICES DIVISION DIRECTOR

In recent weeks the Kansas Bureau of Investigation (KBI) has received several questions about how to submit civil failure to appear arrests to the Central Repositories for Kansas Incident Based Reporting and Criminal History. The Central Repositories are not mandated to track civil cases, only criminal cases. Civil failure to appear should not be reported.

NEW KCJIS NEWSLETTER PUBLISHER

Alicia Madison will be the new contact for the KCJIS Newsletter. You will be receiving the email requesting articles from her starting with the February 2015 Newsletter. Her contact information is alicia.madison@kbi.state.ks.us and 785-296-3302.



KBI

Alicia Madison
1620 SW Tyler
Topeka, KS 66612

Phone: 785-296-3302
Email: alicia.madison@kbi.state.ks.us

The KCJIS NEWSLETTER is published by the Kansas

Criminal Justice Coordinating Council

Derek Schmidt
Chairman
Attorney General

Sam Brownback
Vice Chair
Governor

Council Members:

Kirk Thompson, Director
Kansas Bureau of Investigation

Justice Nancy Moritz,
Chief Justice Designee

Ray Roberts, Secretary of
The Kansas Department of Corrections

Ernest Garcia, Superintendent of
The Kansas Highway Patrol

Brant Laue,
Governor Designee

Lee Davidson, Attorney
General Designee